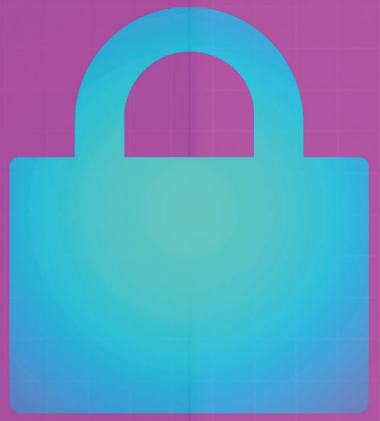
e-bog

datto
A Kaseya COMPANY



Rapport om Dattos SMV-cybersikkerhed for MSP'er

En verden af muligheder for MSP'er

Små og mellemstore virksomheder (SMV'er) står over for stigende cybersikkerhedsudfordringer, hvilket resulterer i, at mange SMV'er øger deres engagement i sikkerhed og deres sikkerhedsbudgetter. Der er plads til, at MSP'er kan realisere indtægtsstigning på mange områder, herunder sikker identitets- og adgangsstyring, slutpunktssikkerhed, forretningskontinuitet og gendannelse efter en katastrofe samt phishingbeskyttelse. Cybertrusler er et voksende problem for SMV'er, hvilket betyder stigende sikkerhedsforretningsmuligheder for MSP'er i hele verden.

Vi talte med 2913 IT-beslutningstagere for at høre om deres sikkerhedsproblemer, og vi deler disse data med dig for at hjælpe dig med at få din MSP til at vokse.

7 Vigtigste konklusioner

IT-fagfolk er bekymrede for sikkerhed og klar til at foretage investeringer for fortsat at sikre deres organisationer.

SMV'er oplever fortsat betydelige sikkerhedsudfordringer, og de anerkender, at de skal bruge penge på at løse dem, og omkring halvdelen af vores respondenter planlægger at bruge penge på e-mailsikkerhed, sikkerhedskopiering og virusbeskyttelse.

Mange SMV'er har brug for hjælp til at forberede sig på at komme sig efter sikkerhedshændelser.

Mere end halvdelen af svarpersonerne i vores undersøgelse indrømmede, at et vellykket phishingangreb eller endnu værre, et ransomwareangreb, ville skade deres organisation alvorligt, og nogle sagde, at det kunne være dødsstødet.

Få SMV'er skærer ned på sikkerhedsudgifter. I stedet investerer de i sikkerhed.

Fire ud af 10 af vores respondenter i undersøgelsen sagde, at deres organisation øger udgifterne til cybersikkerhed, og de fleste forventer, at det fortsætter – fremragende nyt for MSP'er i dagens udfordrende økonomi.

Phishing er det største sikkerhedsproblem, SMV'er står over for.

Virksomheders IT-ledere er bekymrede for phishing og den fare, det bringer med sig. Dette skaber muligheder for indtægtsstigning for MSP'er omkring e-mailsikkerhed og sikkerhedstræning med phishingsimuleringer.

Nedetid er dyrt, men mange virksomheder har ikke de rigtige værktøjer til at minimere det.

MSP'er har en gylden mulighed for at udvide indtægter og hjælpe deres kunder med at reducere dyr nedetid med løsninger som BCDR, administreret SOC og hændelsesreaktionsplanlægning.

SMV'er har en tendens til at stole på udliciteret IT-sikkerhed.

Virksomheder har brug for hjælp udefra for at opretholde og forbedre deres sikkerhed, og næsten halvdelen af de IT-fagfolk, som vi undersøgte, sagde, at deres organisation er afhængig af en MSP eller MSSP for at få arbejdet udført.

En lang række SMV'er er ikke tilfredse med deres nuværende forsvarspakke.

En tredjedel af vores svarpersoner sagde, at de er utilfredse med deres nuværende udvalg af sikkerhedsløsninger, hvilket indikerer, at der er plads til, at MSP'er kan manøvrere på markedet.

Cybersikkerhedsrammeværk

NIST er ikke det mest populære rammeværk

Nultillid anbefales stærkt af eksperter, men kun 14 % af svarpersonerne sagde, at deres organisationer bruger rammeværket, og kun 7 % var bekymrede om det, hvilket giver masser af plads til vækst (og muligheder for MSP'er) på dette område.

Rammeværk eller regulering	Brugsniveau	Bekymringsniveau
CIS	34 %	26 %
CMMC	30 %	26 %
COBIT	27 %	23 %
NIST	22 %	19 %
ISO 27001	21 %	15 %
NCSC (National Cyber Security Centre)	18 %	20 %
HIPAA	18 %	13 %
Zero Trust	14 %	7 %
ASD Essential 8	14 %	13 %
PCI-DSS	12 %	10 %
SOC II	11 %	7 %
MITRE ATT&CK	9 %	9 %
Andet	5 %	Ikke tilgængelig
Ingen	3 %	27 %

CIS og CMMC bruges oftest og er de mest bekymrende cybersikkerhedsrammeværker.

SMV'er er proaktive med hensyn til at vurdere sårbarheder

Størstedelen af SMV'er i alle regioner er interesserede i at holde øje med deres IT-sikkerhedssårbarheder i et så ustabilt cyberkriminalitetsklima. Det gør dem særligt ivrige efter brugervenlige løsninger, der gør sårbarhedsvurderingsprocessen hurtig og nem.

Hyppighed af vurderinger	Svar
Mere end fire gange om året	13 %
Tre til fire gange om året	24 %
To gange om året	25 %
Én gang om året	21 %
Én gang hvert 2.-4. år	12 %
Én gang hvert 5. år eller længere	3 %
Aldrig	1 %
Ved ikke	2 %

Over en tredjedel af svarpersonerne udfører IT-sikkerhedssårbarhedsvurderinger tre eller flere gange om året.

SMV'er skærer ikke ned på sikkerhedsudgifterne; budgetterne stiger i stedet

På grund af stigende cyberkriminalitet og en voksende bevidsthed om de skader, et cyberangreb kan gøre blandt beslutningstagere for ikke-teknologiske anliggender, er IT-sikkerhedsbudgetterne steget i det forløbne år. SMV'er er optimistiske om, at de forbliver stabile eller stigende i 2023. Dette giver MSP'er mulighed for at opfordre kunderne til at foretage omfattende sikkerhedsforbedringer og -opgraderinger.

IT-budgetter	Svar
Steget	42 %
Forblev det samme	40 %
Faldet	6 %

Fire ud af 10 (42 %) af svarpersonerne i undersøgelsen rapporterede et øget IT-sikkerhedsbudget i år.

Sikkerhed er en stor del af de fleste IT-budgetter

SMV'er har råd til sikkerhed

% af det samlede IT-budget	Svar
Mindre end 1 %	1 %
1-5 %	10 %
6-10 %	19 %
11-15 %	19 %
16-20 %	20 %
21-30 %	15 %
31-40 %	8 %
41-50 %	5 %
Mere end 50 %	3 %

Næsten en tredjedel af SMV'er afsætter 20 % til 50 % af deres IT-budget til sikkerhed.

SMV'er er på jagt efter IT-sikkerhedshjælp

Mens mange SMV'er håndterer sikkerhed internt, er der masser af virksomheder, der søger MSP'er og MSSP'er til at dække deres IT-sikkerhedsbehov. Mangel på teknisk talent er en medvirkende faktor, men mangel på ekspertise er også en vigtig motivationsfaktor for virksomheder til at udlicitere deres teknologiarbejde. MSP'er kan drage fordel af at positionere sig selv som kyndige, opdaterede eksperter for kunder og potentielle kunder.

En ud af fire udliciterer deres sikkerhed til en MSP, og en ud af seks til en MSSP.

Hvem administrerer din IT-sikkerhed?	Svar
Delvis intern IT	47 %
Dedikeret intern IT	50 %
Individuel udliciteret IT	28 %
Firma udliciterer IT, der er IT-tjenesteudbyder eller MSP	26 %
Virksomheden udliciterer IT, der er en MSSP	16 %
Virksomheden udliciterer IT, men jeg er ikke sikker på, hvilken type det anses for at være	5 %

Der er plads til, at MSP'er på markedet

Kun 31 % af svarpersonerne fortæller os, at de er helt tilfredse med deres sikkerhedsløsninger, hvilket skaber muligheder for, at MSP'er kan vokse.

Tilfredshedsniveau	Svar
Fuldstændig tilfreds	31 %
Rimelig tilfreds	54 %
Neutral	12 %
Rimelig utilfreds	2 %
Meget utilfreds	1 %

Kun 54 %

af virksomhederne er rimelig tilfredse med deres sikkerhedsløsninger.

De fleste virksomheder har forstået budskabet om, at en gendannelsesplan er en forretningsmæssig nødvendighed

Når det kommer til at have en gendannelsesplan på plads, sagde over halvdelen af svarpersonerne, at de har en standardgendannelsesplan klar. Nogle virksomheder har dog stadig brug for stor hjælp til at udarbejde en gendannelsesplan, hvilket skaber muligheder for MSP'er for at hjælpe dem med at være klar, hvis problemerne opstår. Det er også en god mulighed for MSP'er til at vejlede kunder i at investere i de ressourcer, de skal bruge til at gennemføre planen, såsom BCDR eller værktøjer til fjernidentitet og adgangsstyring.

Otte ud af ti respondenter (81 %) sagde, at deres virksomhed har en gendannelsesplan på plads.

Status for gendannelsesplan	Svar
Vi har en gendannelsesplan der er bedst i sin klasse på plads	29 %
Vi har en standardgendannelsesplan på plads	52 %
Vi har løsninger til at beskytte os, men har ikke en formel gendannelsesplan på plads	14 %
Vi har ingen gendannelsesplan på plads	2 %
Jeg mener, at min tjenesteudbyder har en gendannelsesplan på plads, men jeg kender ikke detaljerne	3 %

Sikkerhedsprodukter

Et stærkt forsvar mod ransomware fører til SMV-prioritetslisten

I ransomwareæraen er det ikke overraskende, at antivirussoftware (57 %) og e-mailsikkerhed (53 %) er øverst på virksomhedernes implementeringslister.

De sikkerhedsløsninger, som organisationer implementerer i løbet af de næste 12 måneder

Løsning	Svarpersoner
Antivirussoftware	57 %
Beskyttelse af e-mail	53 %
Sikkerhedskopiering af fil	49 %
Administreret firewall	49 %
Uddannelse i cybersikkerhed for medarbejdere	43 %
Identitets- og adgangsstyring	38 %
Sikkerhedsdriftscenter	28 %
Administreret registrering og svar (MDR)	27 %
Forretningskontinuitet og gendannelse efter en katastrofe (BCDR)	27 %
Hændelsessvar	27 %
Slutpunktsregistrering og svar	25 %
Automatiseret softwarepatch	25 %
Mobil administrationsplatform	23 %
Trusselsopsporing	20 %
Pentest	14 %
Kriminaltekniske undersøgelser	12 %

Kun 43 % af svarpersonerne gennemfører træning i sikkerhedsbevidsthed.

SMV'er er klar til at investere i skyen

På grund af den stigende cyberkriminalitet de sidste par år er virksomheder klar til at investere i skysikkerhed.

Top IT-sikkerhedsområder SMV'er planlægger at investere i inden for de næste 12 måneder

Investeringsområde	Svar
Netværkssikkerhed	47 %
Skysikkerhed	45 %
Cyberforsikring	36 %
Sikkerhed for e-mail-/samarbejdsværktøjer	29 %
Slutpunktsikkerhed	27 %
Vurdering af sårbarhed	26 %
Forretningskontinuitet og gendannelse efter en katastrofe (BCDR)	25 %
Ved ikke	5 %

Netværkssikkerhed og skysikkerhed er de vigtigste områder, der er planlagt at investere i i 2023.

Cybertrusler

SMV'er har en lang række sikkerhedsproblemer

Et nærmere kig på de faktorer, som SMV'er bebrejder for deres sikkerhedsproblemer, kan hjælpe dig med selvsikkert at tale til deres smertepunkter.

Hovedårsager til, at SMV'er føler, at de har haft cybersikkerhedsproblemer

Problem	Svar
Phishing-e-mails	37 %
Ondsindede netsteder/netannoncer	27 %
Svage adgangskoder/adgangsstyring	24 %
Dårlig brugerpraksis/godtroenhed	24 %
Slutbrugerens manglende uddannelse i cybersikkerhed	23 %
Administratorens manglende uddannelse i cybersikkerhed	19 %
Phishingtelefonopkald	19 %
Mangel på forsvarsløsninger (antivirus)	19 %
Utilstrækkelig sikkerhedssupport til forskellige typer brugerenheder	18 %
Forældede sikkerhedspatches	18 %
Manglende midler til IT-sikkerhedsløsninger	17 %
Medarbejderes mistede/stjålne legitimationsoplysninger	17 %
Mangel på ledelsesstøtte angående sikkerhedsløsninger	16 %
Åben adgang til fjernskrivebordsprotokol (RDP)	15 %
Skygge-IT	13 %

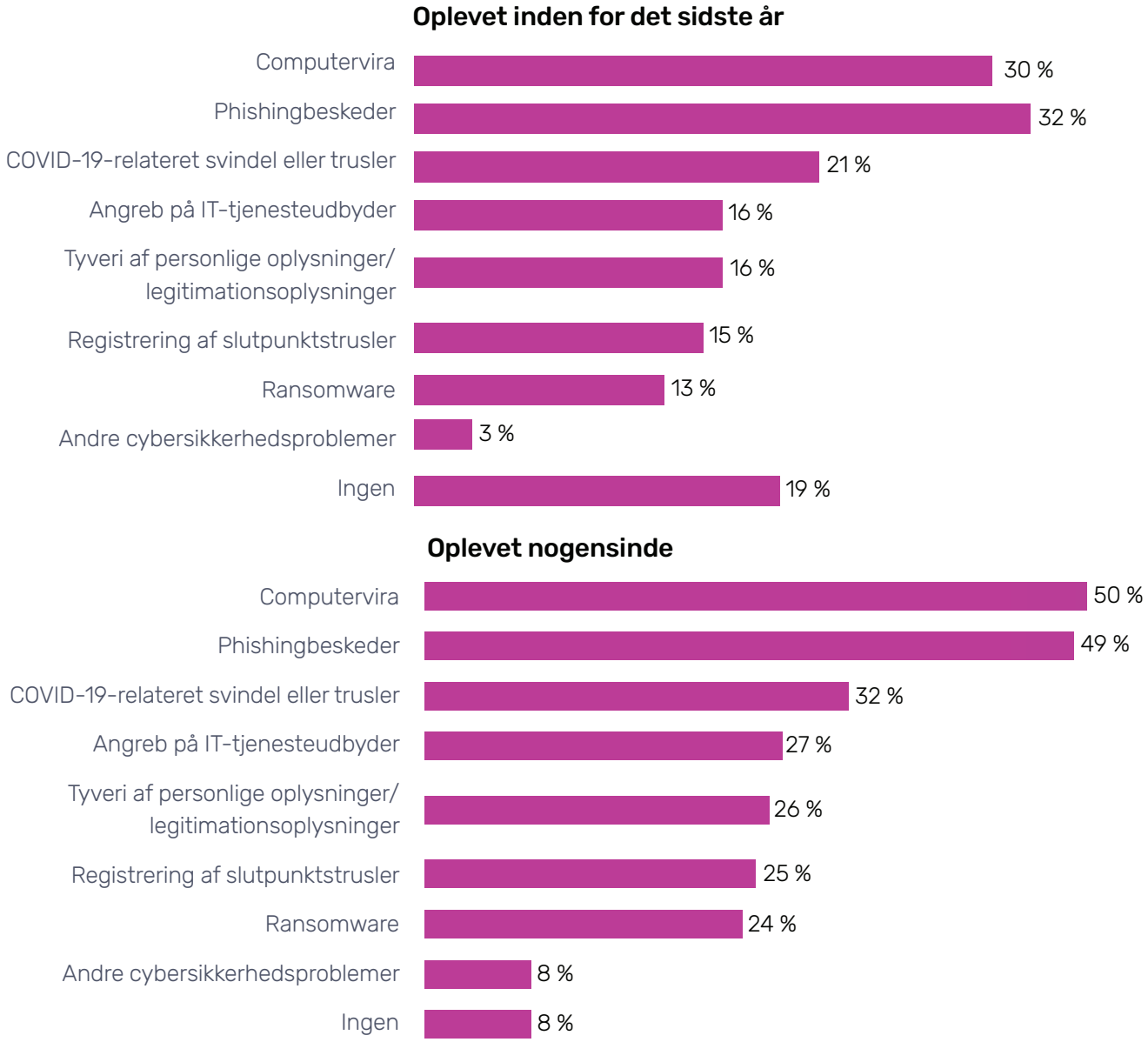
Omkring 42 % af SMV'erne giver manglende uddannelse skylden for deres sikkerhedsproblemer.

SMV'er plages af phishing

Mange af vores svarpersoner så phishing som hovedmistænkt for sikkerhedsproblemer, og mere end en fjerdedel af svarpersonerne har oplevet angreb på deres IT-tjenesteudbyder (16 % i det forløbne år). Dette er en mulighed for MSP'er for at tilbyde en yderst sikker tjeneste.

Cybersikkerhedsproblemer, der har påvirket SMV'ers forretning inden for de sidste 12 måneder.

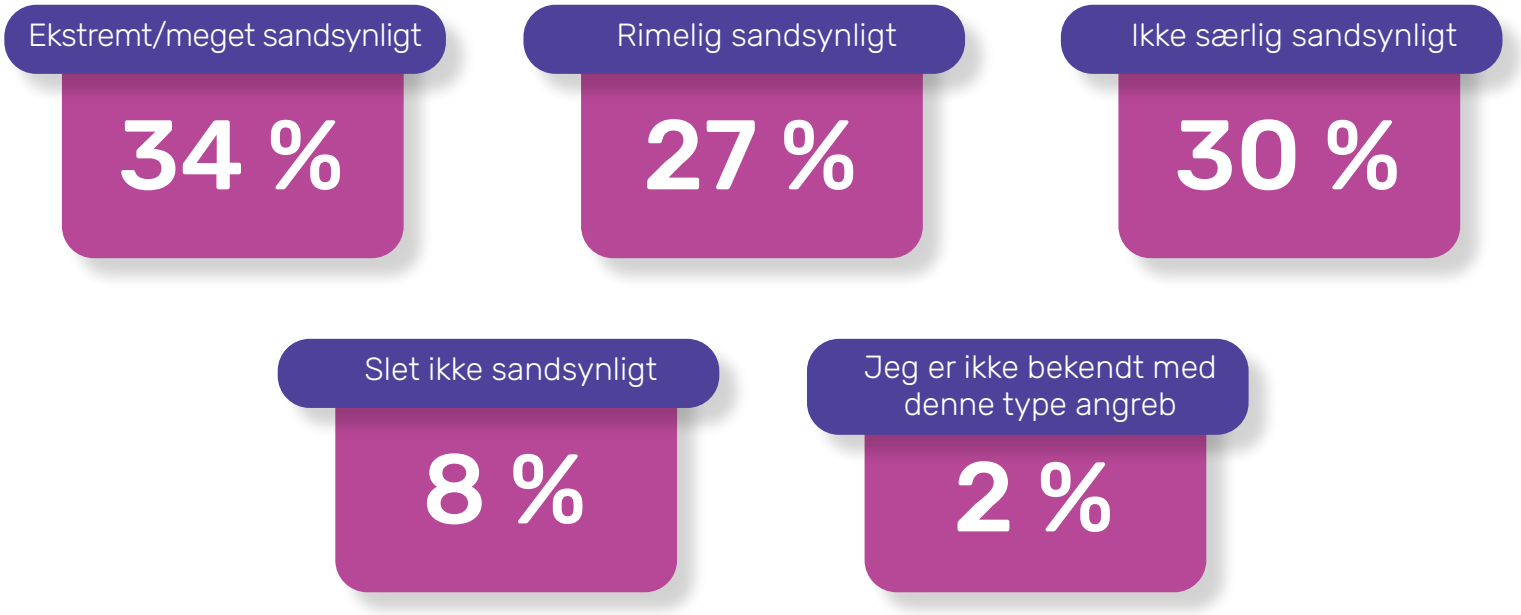
Næsten en tredjedel af svarpersonerne oplevede phishing og vira sidste år.



Næsten tre fjerdedele af virksomhederne siger, at et ransomwareangreb ville være et dødsstød

Virksomheder ved, at et ransomwareangreb kan ødelægge dem, og de leder efter måder at forhindre det på.

Omkring 60 % af svarpersonerne følte, at deres organisation kunne blive ramt af et vellykket ransomwareangreb inden for de næste 12 måneder.



Omkring 70 % af SMV'er indrømmede, at betydningen af et ransomwareangreb ville være voldsom eller væsentlig.

Voldsom betydning – det ville være svært at komme sig

17 %

Væsentlig betydning

53 %

Minimal betydning

28 %

Ingen betydning

3 %

Krav om løsepenge varierer meget

At præsentere kunder og mulige kunder for et klart billede af det løsesumskrav, de kan stå over for, kan hjælpe dem med at forstå de mulige økonomiske konsekvenser.

Næsten en tredjedel af SMV'er oplevede løsesumskrav på $10.000-50.000.

Løsesumsbeløb	Svar
Mindre end $100	2 %
$100 til mindre end $500	4 %
$500 til mindre end $1.000	10 %
$1.000 til mindre end $5.000	21 %
$5.000 til mindre end $10.000	25 %
$10.000 til mindre end $25.000	20 %
$25.000 til mindre end $50.000	11 %
$50.000 eller mere	6 %

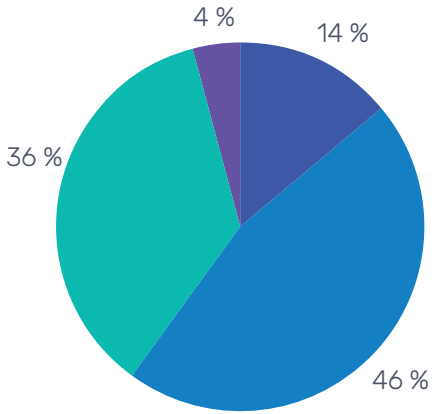
De fleste SMV'er forventer at blive phishet

Lige under tre fjerdedele af svarpersonerne mener, at det er sandsynligt, at deres organisation vil opleve et phishingangreb i det næste år, og også her leder de efter måder at mindske denne risiko på.

Omkring 72 % af svarpersonerne forventer et phishingangreb i løbet af det næste år.

Sandsynlighed	Svar
Ekstremt/meget sandsynligt	41 %
Rimelig sandsynligt	31 %
Ikke særlig sandsynligt	22 %
Slet ikke sandsynligt	7 %

Flere svarpersoner følte, at de ville blive offer for phishing end ransomware det næste år, men de troede, at betydningen af et vellykket ransomwareangreb ville være større for deres organisation end virkningen af et phishingangreb.



Næsten halvdelen af svarpersonerne mener, at et phishingangreb vil have en betydelig indvirkning på deres forretning.

- Minimal betydning
- Væsentlig betydning
- Voldsom betydning – det ville være svært at komme sig
- Ingen betydning

SMV'er har tillid til deres evne til at komme sig efter en cybersikkerhedshændelse

På trods af dette er der rig mulighed for, at MSP'er på dette område kan foreslå nye løsninger, der minimerer risici eller opgraderinger til en kundes eller en mulig kundes sikkerhedsopbygning for at gøre det endnu stærkere – 16 % af svarpersonerne fortalte os, at deres organisation ville være dødsdømt i tilfælde af et vellykket cyberangreb eller anden skadelig cybersikkerhedshændelse, og 47 % sagde, at de mener, at gendannelse ville være vanskelig.

Vellykket gendannelse efter en katastrofe er lettere sagt end gjort

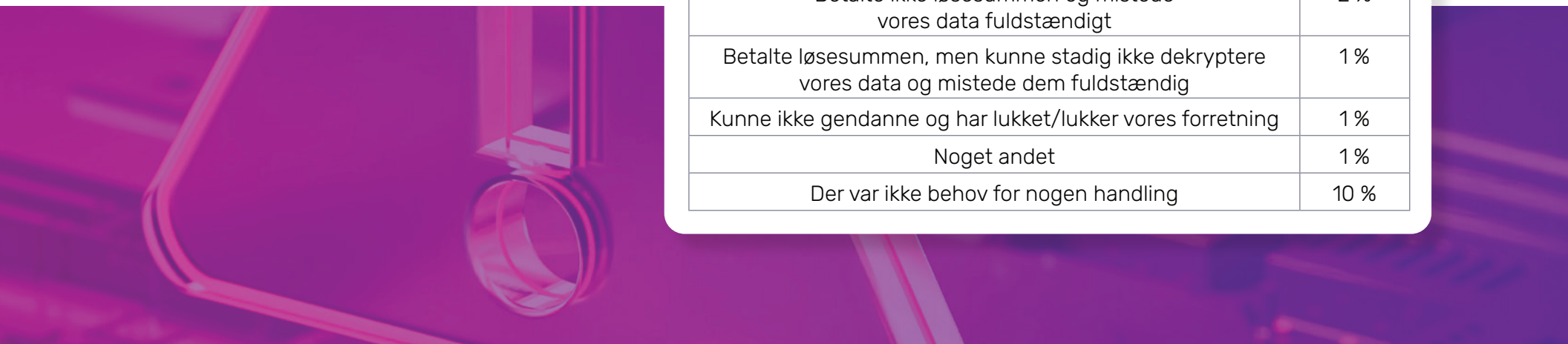
MSP'er kan give SMV'er den hjælp, de har brug for til at forbedre deres sikkerhedskopierings- og gendannelsesprocesser.

En femtedel af svarpersonerne blev tvunget til at geninstallere og omkonfigurere alle systemer fra bunden for at komme tilbage på arbejde.

Lidt under halvdelen af svarpersonerne i undersøgelsen (47 %) sagde, at deres virksomheder sandsynligvis vil komme sig efter et cyberangreb eller en cybersikkerhedshændelse, men det ville være smertefuldt.

Resultat	Svar
Gendannelse ville være let	**37 %**
Gendannelse ville være svært	**47 %**
Vi ville ikke komme os	**16 %**

Handling foretaget for at vende tilbage til udgangspunkt	Svar
Udført gendannelse efter en katastrofe og gendannede alt fra fuldstændige sikkerhedskopieringer	30 %
Gendannede en del af systemerne og geninstallerede og omkonfigurerede resten	29 %
Geninstallerede og omkonfigurerede alle vores systemer fra bunden	21 %
Betalte løsesummen for at få vores data dekrypteret	2 %
Betalte ikke løsesummen og mistede vores data fuldstændigt	2 %
Betalte løsesummen, men kunne stadig ikke dekryptere vores data og mistede dem fuldstændig	1 %
Kunne ikke gendanne og har lukket/lukker vores forretning	1 %
Noget andet	1 %
Der var ikke behov for nogen handling	10 %



Nedetid koster i gennemsnit $126.000

Nedetid er et dyrt problem, som næsten halvdelen af vores svarpersoner kæmpede med i det forløbne år. Den forretningsmæssige betydning og omkostningerne for nedetid giver MSP'er en årsag til at anbefale løsninger, såsom BCDR, der reducerer nedetid i tilfælde af en sikkerhedshændelse. Omkostningerne ved nedetid er også et faktum, der kan bruges, når man taler om sikkerhedskurser og andre forebyggende foranstaltninger.

$126.000 er den gennemsnitlige pris for nedetid, herunder tabt omsætning.

Omkostninger ved nedetid	Svar
$1.000 til mindre end $250.000	84 %
$1.000 til mindre end $250.000	8 %
$1.000 til mindre end $250.000	4 %
$750.000 til mindre end $1 million	3 %
1 million dollars eller mere	1 %

Manuel sikkerhedskopiering er den bedste gendannelsesmetode

Lidt under halvdelen af respondenterne (49 %) sagde, at deres organisationer var afhængige af manuel sikkerhedskopiering for at gendanne data i deres sidste cybersikkerhedshændelse. Det betyder, at halvdelen af de virksomheder, vi undersøgte, skal opdatere til sky-sikkerhedskopiering og lære fordelene ved BCDR – en stor mulighed for MSP'er.

De bedste løsninger eller metoder, der bruges til at gendanne data.

Gendannelsesmetode	Svar
Manuel sikkerhedskopiering	49 %
Kopi fra gamle systemer	36 %
Kontinuerlig tilgængelighed	36 %
BCDR fra tredjepart	32 %
Noget andet	11 %
Vi gjorde ikke noget og gendannede ikke vores data	2 %
Vi mistede ingen data	13 %

Omkring halvdelen af de SMV'er, der havde et cybersikkerhedsproblem, var i gang inden for en dag

I dag hedder det ikke "hvis" du har en hændelse", men "hvornår" og løsninger, der reducerer gendannelsestiden, vil appellere til virksomheder.

Omkring 45 % af virksomhederne havde mere end to dages nedetid.

Gendannelsestid	Svar
Ingen – vi havde ingen nedetid	12 %
Mindre end 1 dag	23 %
1 dag	20 %
2-3 dage	31 %
4-6 dage	10 %
En uge eller mere	3 %
Ved ikke	1 %
Foretrækker ikke at svare	1 %

Cyberforsikring

De fleste SMV'er har eller er på udkig efter cyberforsikring

Svarpersoner med cyberforsikring vil sandsynligvis også deltage i andre smarte sikkerhedspraksisser. De har generelt mere IT-support, flere CSF'er og flere sikkerhedsløsninger implementeret. De er også mere tilbøjelige til at have oplevet en cybersikkerhedshændelse tidligere.

Næsten tre fjerdedele af respondenterne har en cyberforsikring.

En tredjedel af dem uden cyberforsikring er meget tilbøjelige til at investere i det inden for de næste 12 måneder.

Har du en cyberforsikring?

Ja 69 %

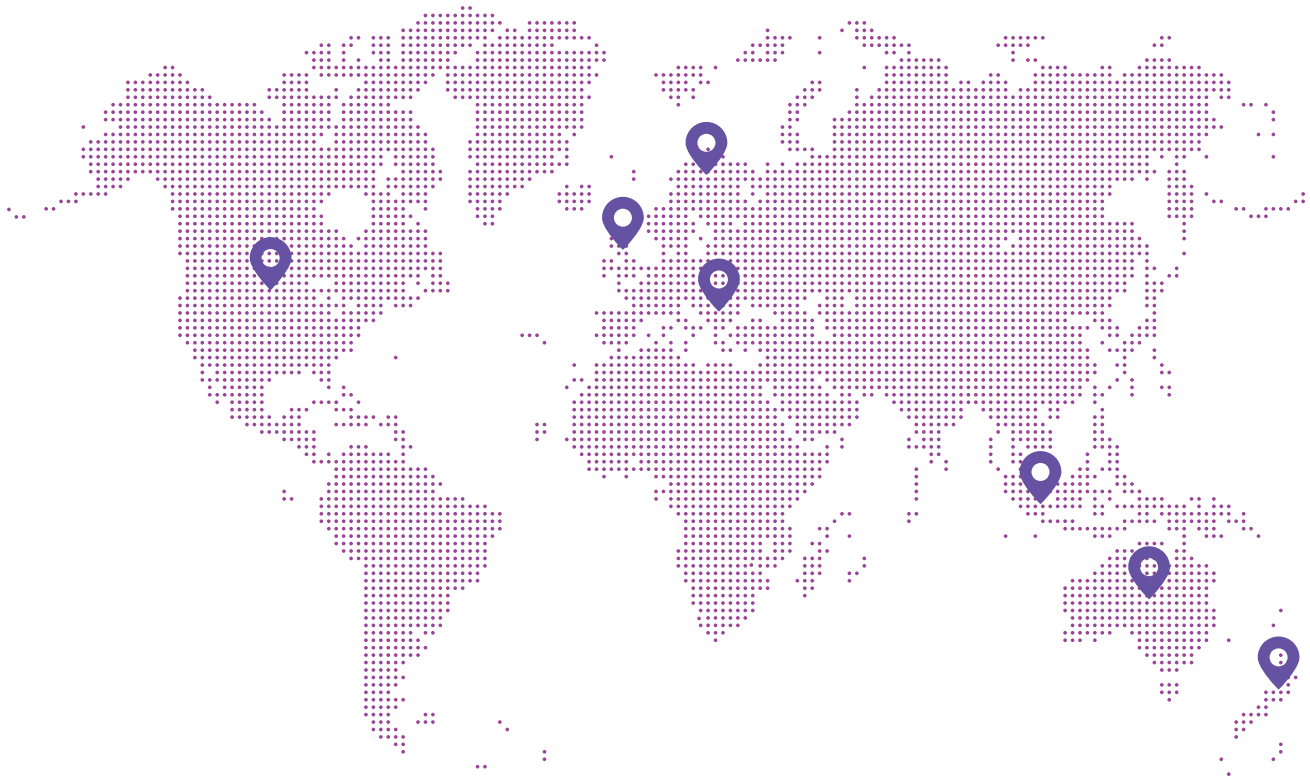
Nej 23 %

Ved ikke 8 %

Sandsynlighed	Svar
Yderst/meget sandsynligt	37 %
Rimelig sandsynligt	38 %
Ikke særlig sandsynligt	22 %
Slet ikke sandsynligt	4 %

Undersøgelsesmetode

Rapporten om Dattos SMV-cybersikkerhed for MSP'er blev oprettet ud fra en delmængde af data indsamlet i en undersøgelse af 2.913 IT-beslutningstagere udført i juli og august 2022. Svarpersonerne skulle være IT-beslutningstager hos en SMV med 10-300 medarbejdere. De markeder, der blev valgt til analyse, var Nordamerika (USA og Canada), Storbritannien, Tyskland, Holland, Australien og New Zealand og Singapore.



Om Datto

Datto, et Kaseya-mærke, der leverer brancheførende skybaserede software- og teknologiløsninger leveret af administrerede tjenesteudbydere (MSP'er). Datto tilbyder Unified Continuity-, netværks- og virksomhedsledelsesløsninger og har skabt et enestående økosystem af MSP-partnere. Disse partnere leverer Datto-løsninger til over en million virksomheder over hele verden. Siden grundlæggelsen i 2007 har Datto hvert år vundet adskillige priser for sit fortræffelige produkt, overlegne tekniske support og hurtige vækst og for at skabe en fremragende arbejdsplads. Med hovedkvarterer i Norwalk, Connecticut, har Datto globale kontorer i Storbritannien, Holland, Danmark, Tyskland, Canada, Australien, Kina og Singapore. Få mere at vide på datto.com.